MSFC-015

"Design for Reliability and Safety" Approach for the New NASA Launch Vehicle

Safie, Fayssal M., Ph.D[1], Weldon, Danny M.[2]

[1] NASA/MSFC, Huntsville Al 35812, fayssal.m.safie@nasa.gov
[2] NASA/MSFC, Huntsville Al 35812, Danny.M.Weldon@nasa.gov:

ABSTRACT

The United States National Aeronautics and Space Administration (NASA) is in the midst of a space exploration program intended for sending crew and cargo to the international Space Station (ISS), to the moon, and beyond. This program is called Constellation. As part of the Constellation program, NASA is developing new launch vehicles aimed at significantly increase safety and reliability, reduce the cost of accessing space, and provide a growth path for manned space exploration. Achieving these goals requires a rigorous process that addresses reliability, safety, and cost upfront and throughout all the phases of the life cycle of the program.

This paper discusses the "Design for Reliability and Safety" approach for the NASA new launch vehicles, the ARES I and ARES V. Specifically, the paper addresses the use of an integrated probabilistic functional analysis to support the design analysis cycle and a probabilistic risk assessment (PRA) to support the preliminary design and beyond.

1.0 BACKGROUND

This section provides some background on the new NASA launch vehicles, and an overview of some of NASA applications of probabilistic methods in recent years.

1.1 NASA New Launch Vehicles

The following paragraphs provide a brief description of the NASA new launch vehicles, ARES I and ARES V. Fig. 1 shows the two vehicles in comparison with themselves and heritage vehicles. The arrows indicate hardware commonality.

The intended purpose of the ARES I, developed by NASA Marshall Space Flight Center (MSFC), is to safely deliver a payload of crew and cargo to a specified ascent target. This capability will support two separate missions: to carry the payloads to the International Space Station (ISS); and to deliver a Crew Exploration Vehicle (CEV) with crew to dock with a Lunar Surface Ascent Module (LSAM) and Earth Departure Stage (EDS) in Earth orbit for a lunar mission.

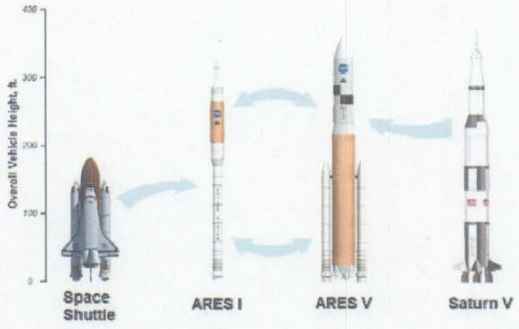

Figure 1. ARES I and ARES V Launch Vehicles in Comparison

The ARES I, shown in Fig. 2, consists of three major Elements: A solid First Stage (FS), an Upper Stage (US), and liquid Upper Stage Engine (USE). The CEV it delivers to orbit consists of a Launch Abort System (LAS), Crew Module (CM), Service Module (SM), and a Spacecraft Adapter (SA). The CEV development is being led by NASA Johnson Space Center (JSC).

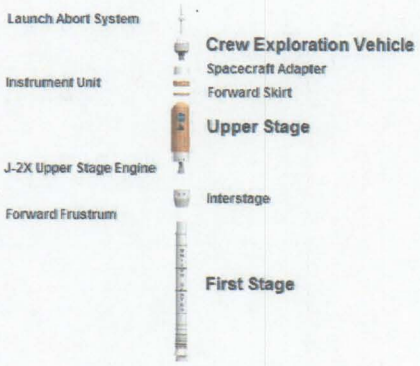

Figure 2. ARES I Expanded View

The intended purpose of the ARES V launch vehicle, also developed by MSFC, is currently to deliver the LSAM for lunar missions, to deliver cargo to orbit, and to potentially deliver a single-launch solution to the Moon with combined CEV and lunar lander payloads. As shown in Fig. 3, the ARES V consists of the following: a liquid Core Stage with 5 RS-68 engines augmented by 2 five-segment Redesigned Solid Rocket Motors (RSRMs); an Interstage; an EDS with payload (LSAM shown); and Shroud.

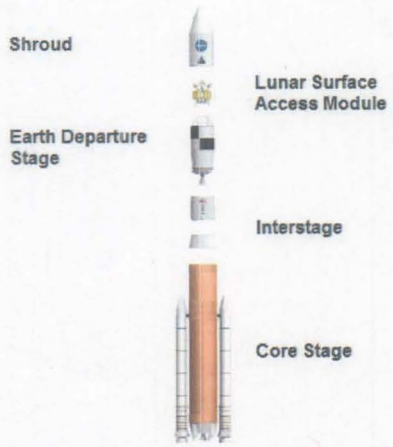

Figure 3. ARES V Expanded View

1.2 Overview of NASA Applications of Probabilistic Methods

Since the Space Shuttle *Challenger* accident in 1986, NASA has begun incorporating Quantitative risk assessments (QRA) in decisions concerning the Space Shuttle and other NASA projects. At MSFC, for example, QRA has been extensively used in areas such as risk management of flight hardware, trade studies, and reliability prediction of new hardware. In the risk management area, life limits based on QRA are being used in the Space Shuttle main engine (SSME) program [1]. QRA has also been incorporated to support flight issues on the SSME as well as other MSFC elements. With regard to trade studies, QRA has been used as the basis to evaluate the elimination of unnecessary inspections, procedures, and other program costs. For example, an extensive study was conducted in 1994 to determine whether to eliminate the pre-proof test x-ray inspections on the Space Shuttle External Tank (ET) [2]. In the reliability prediction area, similarity analysis and probabilistic structural models have been used by MSFC to predict the reliability of Alternate Turbo Pumps (ATD) for the SSME, the X-33 Engine, and other engines [3, 4, and 5].

At the system level, NASA Headquarters has led several studies to predict the overall Space Shuttle risk. The first of these Space Shuttle QRA studies was conducted in 1988 by Planning Research Corporation (PRC). Per NASA's request, PRC conducted a QRA study to determine the Space Shuttle risk for the Galileo mission [6]. In 1993, Science Applications International Corporation (SAIC) updated the Galileo study using Bayesian techniques [7]. In 1995, SAIC conducted a comprehensive QRA study [8]. In July 1996, the NASA Administrator requested an independent QRA to be conducted by NASA QRA experts. In response to the Administrator's request, NASA conducted a two year study (October 1996 - September 1998) to develop a model that provided an overall Space Shuttle risk and estimates of risk changes due to proposed Shuttle upgrades [9]. Finally, building on previous Shuttle risk assessment studies, JSC has recently completed an extensive study of the Space Shuttle risks. This study have not yet officially been released.

After the Columbia accident, NASA conducted a QRA on ET foam. This study was the most focused and most extensive risk assessment that NASA has conducted in recent years. It used a dynamic, physics based, integrated system analysis approach to understand the integrated system risk due to ET foam loss in flight [10].

Unfortunately, a lot of NASA probabilistic analyses in the past have been done after the fact (operational Shuttle system). This paper describes NASA application of probabilistic analysis methods starting at the design phase. Specifically, the paper addresses the use of an integrated probabilistic functional analysis upfront to support the system Design Analysis Cycle (DAC) and a probabilistic risk assessment (PRA) to support the preliminary design and beyond.

2.0 THE "DESIGN FOR RELIABILITY AND SAFETY APPROACH"

The "Design for Reliability and Safety" discussions in this paper is focused on ARES I launch vehicle. However, the same approach is applicable to the ARES V launch vehicle.

Before getting into the discussion of the subject of this paper, it important note the Constellation Program has in place ambitious quantitative requirements for Loss of Mission (LOM) and Loss of Crew (LOC. The LOM and LOC (or equivalents) have been allocated to the ARES I and its major elements, the First Stage (FS), the Upper Stage (US), and the Upper Stage Engine (USE). Satisfying these requirements constitute an ambitious goal that forced a paradigm shift at NASA. This paradigm shift has set the stage for establishing a working environment that integrates various disciplines (safety, reliability, design, etc.) and various organizations (Engineering design organizations, project office, and safety and mission assurance organisation) to support the design process. Within this integrated environment, this paradigm shift has also set the stage for a new era at NASA in applying a sound probabilistic design approach, to analyze, understand, and influence the design upfront and throughout the different phases of the design. This paper focuses on the probabilistic design approach, and more specifically, on the use of the various quantitative probabilistic approaches that have been pursued by the ARES I project.

Section 2.1. discusses an integrated functional probabilistic analysis approach that addresses upfront some key areas to support the ARES I Design Analysis Cycle (DAC) pre Preliminary Design (PD) Phase. This functional approach is a probabilistic physics based approach that combines failure probabilities with system dynamics and engineering failure impact models to identify key system risk drivers and potential system design requirements. Section 2.2 discusses other probabilistic risk assessment approaches planned by the ARES I project to support the PD phase and beyond.

2.1 The Probabilistic Functional Failure Analysis (PFFA) Approach

The PFFA approach is a dynamic top-down scenario-based approach intended to identify, model, and understand high system risk drivers for the purpose of influencing both system design and system requirements. This approach is implemented upfront during the system DAC phase preceding the preliminary design review (PDR). The current focus for the ARES I PFFA is on energetic or dynamic events and significant changes of state for the launch vehicle that can lead to LOM or LOC. Failures not initiated by the launch vehicle, other than those induced by the natural environment, and launch vehicle software failures were not currently considered. The launch vehicle was assumed to be fully tested and qualified with all tests and verification complete.

The first step in a PFFA is to define the mission timeline of system level functions. The applicable ARES I mission timeline includes the pre-launch and ascent phases. The system level functions during the phases include fuel load, crew load, pre-start, launch, staging (FS separation and USE start), LAS jettison, Main Engine Cutoff (MECO), and orbit insertion (payload separation) with CEV separation from the Upper Stage. Fig. 4 shows the ARES I ISS ascent mission profile including elapsed times.

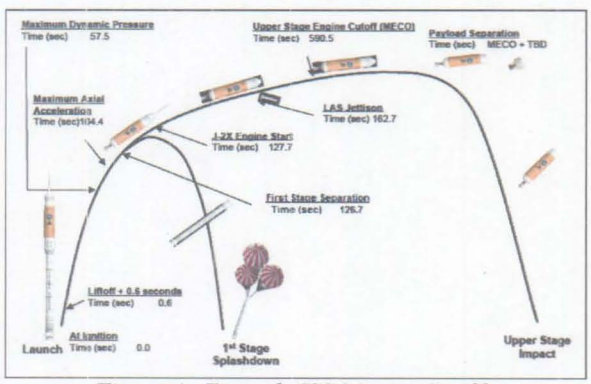

Figure 4. Example ISS Mission Profile

Given the mission timeline of system level functions, the next step in a PFFA is to identify for each system level function the lower-level functions to a selected level of indenture. These lower-level functions are then transformed into a failure structure by restating each as functional failure or failure event. Next, the functional failures are analyzed for their effects on the applicable physical design. The resulting failure effects, labeled as hazards or undesired conditions, are grouped by commonality of their effect on element (e.g., Upper Stage) or launch vehicle. These groupings are labeled as failure bins which are listed for further analysis. Tab. 1 is an example of such a failure bin for the uncontained (energetic failure with hazardous physical effects crossing beyond the source boundary) failure of the Upper Stage Engine.

Table 1. Example of a Bin for Upper Stage Engine Uncontained Failure

Failure Events or Scenarios	Hazard or Undesired Condition
MFV fails to open	Ox-rich combustion in MCC. LOC
Insufficient purge at igniter on	Trapped propellants ignite/explode
Insufficient purge at igniter on	Trapped propellants ignite/explode
Excessive gas spin flow	Excess propellant flow to engine. Overpressure in MCC/GG. If not detected, rupture and LOC
GGFV fails to open	Lox-rich combustion in GG. Fire/explosion. LOC
Excessive gimbaling during engine start	Structural Damage
Engine Hardware failure	Fire/explosion
MCC/Nozzle burnthrough	Hot gas impingement on engine. LOC
Nozzle extension burnthrough	Side thrust. If TVC unable to correct for thrust enough to give time for crew abort, LOC. Otherwise LOM
Seal failure	Hot gas impingement on engine. LOC
MCC/GG overpressure data not relayed to/from engine	Continued MCC overpressure results in rupture. LOC
Insufficient propellant (NPSP) from US to engine (either LO2 or LH2)	Engine cavitation leading to uncontained failure LOC.
Insufficient propellant quality/volume (gas) from US to engine	Engine turbopumps could overspeed
Insufficient propellant (NPSP) from US to engine	Engine cavitation

Given the list of failure bins, the next step in a PFFA is to determine the "bounding" failure scenario for each bin. The "bounding" failure scenario is selected based on the frequency of occurrence, the impact on system risk, and the potential for design improvement.

Given the "bounding" failure scenarios, a short list (a handful of scenarios) is established based on project priorities for further in-depth focused analysis. Specifically, the items on the short list are subjected to in-depth physics based dynamic simulation modeling to understand the physics of failure, the probability of launch vehicle failure or break up, and the launch abort system capability to save the crew. Fig. 5, Fig. 6, and Fig. 7 represent an end-to-end example of the logic of the components of the in-depth focused analysis for an item that could potentially be part of the short list for ARES I.

Fig. 5 shows a representation of the path and off-nominal time from the failure event, labeled "initiator", to the physical failure mode of rupture, labeled "fault", to the local failure effects, labeled "threat/hazardous environment", from which the crew must escape. Each failure event or initiator is assumed to cause an immediate loss of mission and a decision to perform an abort.

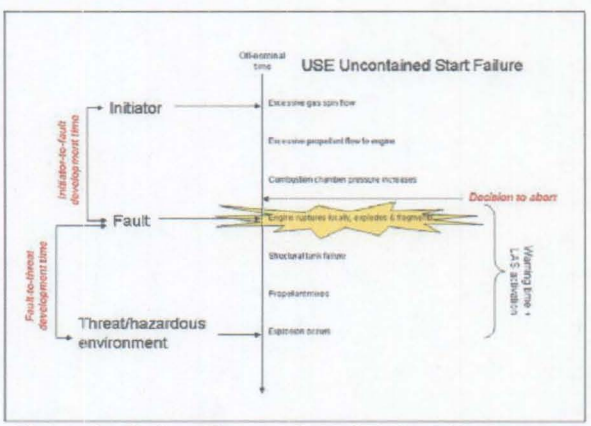

Figure 5. Failure Event to Initial Failure Environment Example

Fig. 6 shows an example of the failure logic for an explosion resulting from the energetic event of an USE uncontained start failure as seen in the previous figure. Hazards to other launch vehicle elements from an explosion include overpressure, fragmentation, and fire. Physics-based simulation models will be developed for each hazard to crew survivability as applicable. For example, the model for overpressure risk to crew will involve a blast model that makes use of the equivalent TNT yield of the liquid propellant, launch vehicle trajectory and flight environment data, physical parameters of the LAS and crew module, other critical ascent and launch vehicle parameters, and LAS activation time.

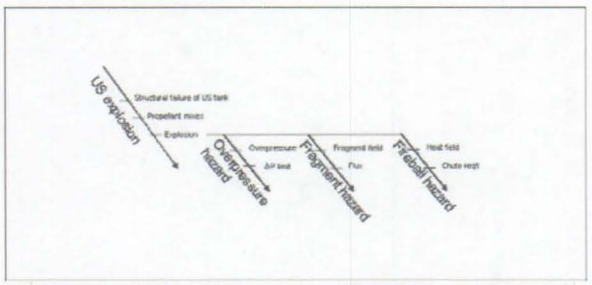

Figure 6. Failure Environment Development Example

Fig. 7 illustrates the combined failure timeline from initiator to critical overpressure for the example scenario along with a crew escape timeline. The crew escape timeline is superimposed upon the failure timeline to model the effectiveness of abort capability against the particular hazard to crew. The escape timeline involves the response and abort capability of the LAS and CEV. It includes detection of the hazard, activation of the LAS, and subsequent CEV separation to a safe position.

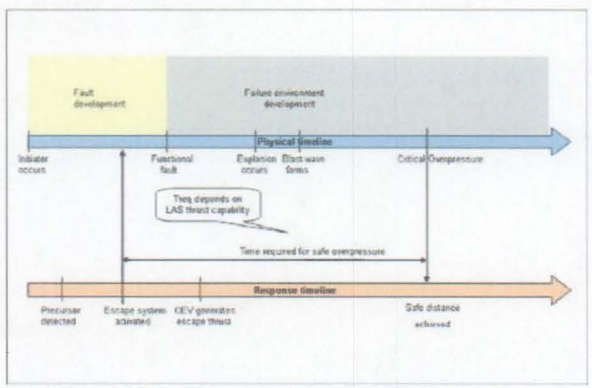

Figure 7. Failure and Crew Escape Timeline

To summarize, the process just described in the example (Fig. 5, Fig. 6, and Fig. 7) starts with a failure initiators, followed by propagations of the failure initiator to a system failure, and then the impact of the system failure on the LOC. This all done taking into consideration the system dynamics at the time of the failure initiation and the physics of the failure as the failure propagates through the system all the way to the impact of the failure on the effectiveness of the abort system.

While the PFFA described in section 2.1 serves the purpose of impacting the design during the system DAC, a classical PRA is performed subsequently to support the preliminary design, detailed design and beyond. The PRA would be structured and focused by the results of the PFFA. The following section discusses the classical PRA process that will be used in

conjunction with the PFFA to support post DAC design phases.

2.2. The PRA Process

PRA is a rigorous method to model what can go wrong with a system, predict how often it might go wrong (the probability that specific undesired events will occur), identify the consequences if something does go wrong, and, engage the design and development community to the fullest extent. Within NASA the PRA uses as input, among others, the safety, reliability, and even quality models and analyses. These would include hazard analyses, fault tree analyses, failure modes and effects analyses, reliability predictions, and process characterization and control analyses. PRA provides information on the uncertainty of the predictions and identifies which failures and, therefore, which systems, subsystems, and components, pose the most significant risk to the system. The following is a description of the PRA process as defined by NPR 8705.5, Probabilistic Risk Assessments (PRA) Procedures for NASA Programs and Projects.

Fig. 8 shows a generic PRA process. The master logic diagram (MLD) is a hierarchical, top-down display of initiating events (IE), showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers, and displaying initiating events at the bottom. The modeling of each accident scenario proceeds with inductive logic tools called event sequence diagrams (ESDs). An ESD starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events called pivotal events, until an end state is reached. ESDs are mapped into event trees (ETs), which relate more directly to practical quantification of accident scenarios, but the ESD representation has the significant advantage over the ETs of enhancing communication between risk engineers, designers, and crews. Upon completion of the event trees, Fault Trees (FTs) are created to model how failures and other events combine to cause failures of pivotal events (intermediate events) in the accident scenario. The pivotal events are placed at the tops of the FTs and deductive logic is used to identify the combination of events that may result in the top event—i.e., to develop the branches of the fault trees. The fault trees may consist of: the top event (pivotal event), intermediate events or logic gates, and the basic events. The basic events are linked to the top event through the intermediate logic gates. The fault trees are simplified through Boolean reduction to quantify each pivotal event in the scenario. The accident sequences (event sequences) and FTs are logically linked and quantified, usually using an integrated PRA computer program. The frequency of occurrence of each end state in the ET is calculated as the product of the IE frequency and the (conditional) probabilities of the pivotal events along the scenario path linking the IE to the end state. Scenarios are grouped according to the end state of the scenario defining the consequence. All end states are then grouped, i.e., their frequencies are summed up into the frequency of a representative end state. As part of the quantification, uncertainty analyses are performed to evaluate the degree of knowledge or confidence in the calculated numerical risk results. [11]

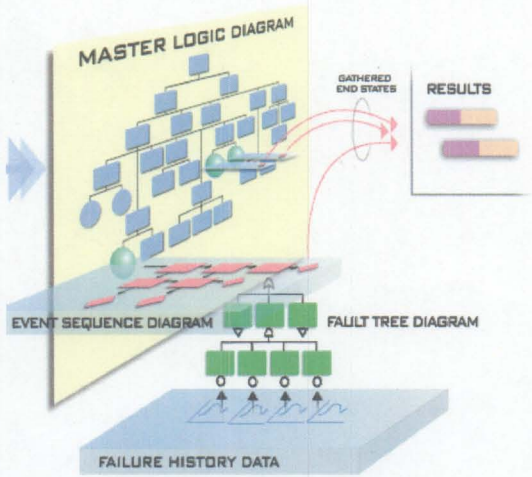

Figure 8. PRA Process

2.2.2 PFFA and PRA in support of the Design process

As discussed in section 2.1, the intent of the PFFA is to analyze and understand a set of integrated system failure scenarios that have the major impact on system risk. The analysis results are then used for potential design changes, abort requirements changes, fault detection improvements, and possibly design changes to reduces or eliminate the probability of the failure initiator. The analysis in a PFFA is dynamic in nature. It takes into consideration the dynamic of the failure sequence as a function of time, and the dynamics of the system environment. On the other hand, the PRA described in the above section is, generally, static in nature. While the PFFA serves the purpose of impacting the design during the system DAC, a classical PRA is performed subsequently to support the preliminary design, detailed design and beyond. The PRA would be structured and focused by the results of the PFFA. Specifically, the PFFA work results in the event sequence diagrams and possibly the initial event trees and branch point quantification that would be part of the PRA. These models would then be supplemented by detailed fault tree models and supporting data analyses, as required, in the areas that have been shown in the PFFA as the potential risk drivers.

3.0 CONCLUSION

The authors of this paper tried to describe a changing environment at NASA set by a paradigm shift on how NASA is planning to use probabilistic assessment methods to support the design process for its new launch vehicles. The PFFA discussed in the paper represents a critical first step for the implementation of a "design for Reliability and Safety" approach needed for achieving the NASA ambitious goals in designing a highly reliable and safe launch vehicles.

4.0 ACKNOWLEDGEMENT

The authors of this paper would like to acknowledge the ARES I abort risk assessment team at MSFC, JSC, and ARC for their contribution to material used to write this paper. Special acknowledgement is made to risk and reliability expert Professor Joe Fragola, Vice President, Valador, Incorporated, for his contribution to the PFFA activity across the various NASA Centers.

5.0 REFERENCES

1. Safie F.M., *A Statistical Approach for Risk Management of Space Shuttle Main Engine Components.* Probabilistic Safety Assessment and Management, 1991
2. Safie F.M., *A Risk Assessment Methodology for the Space Shuttle External Tank Welds*. Reliability and Maintainability Symposium, 1994.
3. Hoffman C.R., Pugh R., Safie F.M., *Methods and Techniques for Risk Prediction of Space Shuttle Upgrades*. AIAA, 1998.
4. Fox E.P., *SSME Alternate Turbopump Development Program*—Probabilistic Failure Methodology Interim Report. FR-20904-02, 1990.
5. Safie F.M., Fox E.P., *A Probabilistic Design Analysis Approach for Launch Systems*. AIAA/SAE/ASME 27th Joint Propulsion Conference, 1991.
6. Planning Research Corporation, *Independent Assessment of Shuttle Accident Scenario Probabilities for Galileo Mission and Comparison with NSTS Program Assessment*, 1989.
7. Science Applications International Corporation, *Probabilistic Risk Assessment of the Space Shuttle Phase 1: Space Shuttle Catastrophic Failure Frequency Final Report*, 1993.
8. Science Applications International Corporation, *Probabilistic Risk Assessment of the Space Shuttle*, 1995
9. Safie F. M., *An Overview of Quantitative Risk Assessment for the Space Shuttle Propulsion Elements*, The fourth Probabilistic Safety Assessment and Management (PSAM4), NY City, 1998.
10. Safie F.M., *Role of Process Control in Improving Space Vehicle Safety A Space Shuttle External Tank Example*, 1st IAASS Conference "Space Safety, a New Beginning, Nice, France, 2005.
11. NPR 8705.5, *Probabilistic Risk Assessments (PRA) Procedures for NASA Programs and Projects.*